

2.D.1 Statement by the Submitter

I, Marshall C. Phelps, Jr. do hereby declare that to the best of my knowledge the practice of the algorithm, reference implementation, and mathematically optimized implementations, I have submitted, known as MARS may be covered by the following U.S. and/or foreign patents: None.

I do hereby declare that the following pending patent applications may cover the practice of my submitted algorithm, reference implementation or mathematically optimized implementations: IBM application CR998021.

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Advanced Encryption Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for inclusion in the Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES). I further understand that I will not receive financial compensation from the government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the AES or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for inclusion in the AES, I hereby agree not to place any restrictions on the use of the algorithm intending it to be available on a worldwide, non-exclusive, royalty-free basis.

I do hereby agree to provide the statements required by sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover practice of my algorithm, reference implementation or mathematically optimized implementations and the right to use such implementations for the purposes of the AES evaluation process.

I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for inclusion in the FIPS (including those not selected for second round of public evaluation), I understand that all rights, including use rights of the reference and mathematically optimized implementations, revert back to the submitter (and other owner[s] as appropriate). Additionally, should the U.S. Government not select my algorithm for inclusion in the AES after a period of four years from the close of the submission date for candidate algorithms, all rights revert to the submitter (and other owner[s] as appropriate).

Signed: 

Title: Vice President, Intellectual Property & Licensing

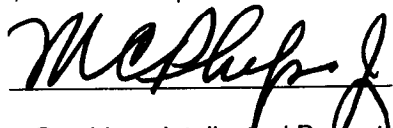
Dated: April 28, 1998

Place: Thornwood, NY

2.D.2 Statement by Patent (and Patent Application) Owner(s)

I, Marshall C. Phelps, Jr., of IBM, 500 Columbus Avenue, Thornwood, NY 10594, am the owner or authorized representative of the owner (International Business Machines Corporation) of the following patent(s) and or patent application(s): IBM application CR998021, and do hereby agree to grant to any interested party if the algorithm known as MARS, is selected for inclusion in the Advanced Encryption Standard, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the mathematically optimized implementations. Furthermore, I agree to grant the same rights in

any other patent granted to me or my company which may be necessary for the practice of the referenced algorithm, reference implementation, or the mathematically optimized implementations.

Signed: 

Title: Vice President, Intellectual Property & Licensing

Dated: April 28, 1998

Place: Thornwood, NY

2.D.3 Statement by Reference/Mathematically Optimized Implementations' Owner(s)

I, Marshall C. Phelps, Jr., am the owner or authorized representative of the owner (International Business Machines Corporation) of the submitted reference implementation and mathematically optimized implementations and hereby grant the Government and any interested party the right to use such implementations for the purposes of the AES evaluation process notwithstanding that the implementations may be copyrighted.

Signed: 

Title: Vice President, Intellectual Property & Licensing

Dated: April 28, 1998

Place: Thornwood, NY

Permission and Author's Copyright Release

I, NEVENKO ZUNIC
(~~insert name of submitter~~), do hereby grant to the National Institute of Standards and Technology (NIST) the nonexclusive right to reproduce or to have reproduced, prepare or have prepared in derivative form, and distribute or have distributed copies of

(check one)

(☒) all materials submitted to NIST in my Advanced Encryption Standard candidate nomination

-- OR --

(☐) all materials submitted to NIST in my Advanced Encryption Standard candidate nomination EXCEPT (enumerate and describe; please submit copyright waivers for these materials signed by the copyright owner or remove from submission package):

I also represent that the exercise of these rights by NIST will not infringe or otherwise violate any rights of another person or organization.

Agreed to and Accepted

Nevenko Zunic
Signature of Submitter

Printed Name: NEVENKO ZUNIC

Title: PROGRAM MANAGER

Organization: IBM

Date: 6/2/98



Office of the Vice President, Intellectual Property & Licensing Services

500 Columbus Avenue, Thornwood, New York 10594

April 28, 1998

Mr. Stuart W. Katzke
NIST North (820), Room 427
Gathersburg, MD 20899

Dear Mr. Katzke:

IBM is pleased to respond affirmatively to NIST's "Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)." As you know, IBM is concerned that some of the language used in the license agreement pertaining to the AES candidate algorithm submission may be susceptible to more than one interpretation. Thus, the purpose of this letter is to state IBM's understanding of the NIST position and seek NIST's agreement that our understanding of the license language is correct. To that end, I have outlined the areas of concern along with our understanding of what is meant by the language.

1. Section 2.D.1, paragraph 3, sentence 4, contains the words "...I have fully disclosed all patents and patent applications *relating to* my algorithm." We are concerned that there could be many patents which could broadly be considered as "*relating to*" an algorithm which is eventually implemented in software or hardware in a computer. We presume that NIST did not intend that patents in such areas as microelectronics, board circuitry, or operating systems - to name a few - would be included in the patent grant. Therefore, the only patents which are deemed to "relate to" the algorithm are those which have claims which are necessarily infringed by the implementation of the algorithm which was adopted as the AES.

2. With regard to the words "...agree to grant the same rights in any other patent granted...." in Section 2.D.2, last sentence, particularly with respect to possible future patents issued on an improvement, we presume that NIST intended that a grant to such patents would only be required if the improvement is formally submitted to NIST (with a new license grant) during the review period and the improvement is incorporated into or becomes the formal standard. Thus, should an improvement be identified by IBM, formally be submitted to NIST and be incorporated into or become the AES, any patent rights to that improvement would be consistent with IBM's understandings expressed in item 1. That is, the grant would be to patents having claims which are necessarily infringed by the implementation of the improved algorithm in or as the AES.

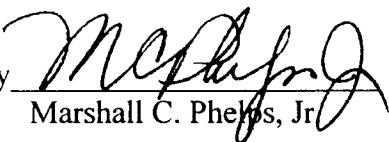
We would appreciate NIST's agreement that our interpretations of the two points above is correct and in accordance with NIST's understandings and intent. If so, please so indicate by having one of the duplicate copies of this letter signed on behalf of NIST and returned to me.

We understand that you might wish to make other potential submitters aware of these interpretations and thus give NIST permission to make this letter available to the public.

Thank you.

Very truly yours,

INTERNATIONAL BUSINESS
MACHINES CORPORATION

By 
Marshall C. Phelps, Jr.

Concurred

NIST
By 